Zestaw 4

1 Funkcja Eulera

Teoria

Jeśli n jest dodatnią liczbą całkowitą, to przez $\varphi(n)$ oznaczamy liczbę elementów zbioru

$$\{a \in [0, n-1] : \gcd(a, n) = 1\},$$

a więc liczbę reszt z dzielenia przez n, które są względnie pierwsze z n. Definiujemy w ten sposób funkcję $\varphi\colon \mathbb{N}_+ \to \mathbb{N}_+$, którą nazywamy funkcją Eulera.

Dla przykładu, gdy $n = 12$, to resztami z dzielenia przez n, które są względnie pierwsze z n, są

$$1, 5, 7, 11,$$

a więc $\varphi(12) = 4$. Zauważmy, że powyższe reszty można znaleźć w następujący sposób: liczbami pierwszymi dzielącymi liczbę 12 są 2 i 3, a więc aby znaleźć reszty względnie pierwsze z 12 trzeba spośród wszystkich reszt, tj.

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11,$$

usunąć te podzielne przez 2

$$\not{0}, 1, \not{2}, 3, \not{4}, 5, \not{6}, 7, \not{8}, 9, \not{10}, 11$$

oraz przez 3

$$\not{0}, 1, \not{2}, \not{3}, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11,$$

co daje powyższą odpowiedź.

Uogólniając powyższą obserwację, otrzymujemy pierwszy wzór na funkcję Eulera: jeśli $p_1, \ldots, p_m$ są wszystkimi parami różnymi liczbami pierwszymi dzielącymi liczbę n, to

$$\varphi(n) = n \cdot \Big(1 - \frac{1}{p_1}\Big) \cdots \Big(1 - \frac{1}{p_m}\Big). \tag{1.1}$$

Jeśli dodatkowo wiemy, że

$$n = p_1^{k_1} \cdots p_m^{k_m}$$

dla dodatnich liczb całkowitych $k_1, \ldots, k_m$ (oraz parami różnych liczb pierwszych $p_1, \ldots, p_m$), to

$$\varphi(n) = p_1^{k_1-1}(p_1 - 1) \cdots p_m^{k_m-1}(p_m - 1) \tag{1.2}$$

oraz

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_m^{k_m} - p_m^{k_m-1}). \tag{1.3}$$

Przykład

Dla $n = 1800$ mamy

$$600 = 2^3 \cdot 3^2 \cdot 5^2,$$

więc korzystając ze wzoru (1.1), otrzymujemy, że

$$\varphi(1800) = 1800\Big(1 - \frac{1}{2}\Big)\Big(1 - \frac{1}{3}\Big)\Big(1 - \frac{1}{5}\Big) = 480.$$

Podobnie, ze wzorów (1.2) i (1.3) otrzymujemy, odpowiednio, iż

$$\varphi(1800) = 2^2(2-1) \cdot 3^1(3-1) \cdot 5^1 \cdot (5-1) = 480$$

i

$$\varphi(1800) = (2^3 - 2^2)(3^2 - 3^1)(5^2 - 5^1) = 480.$$

Odpowiedzi do Zadania 1

(1) 400.

(2) 100.

(3) 48.

(4) 96.

(5) 720.

2 Równania z funkcją Eulera

Teoria

Celem tej części jest przedstawienie metody rozwiązywania równań postaci

$$\varphi(n) = m$$

ze znanym m oraz niewiadomą n.

Metoda opiera się na następujących obserwacjach:

(T1) Ze wzoru (1.2) wynika, że jeśli p jest dzielnikiem pierwszym liczby n, to $p - 1 \mid \varphi(n)$. Powyższa obserwacja pozwala wyznaczyć potencjalne dzielniki pierwsze $p_1, \ldots, p_l$ liczby n.

(T2) Ponieważ $p_1, \ldots, p_l$ są parami różnymi liczbami pierwszymi, więc

$$\varphi(p_1^{k_1} \cdots p_l^{k_l}) = \varphi(p_1^{k_1}) \cdots \varphi(p_l^{k_l}).$$

Zatem musimy wyznaczyć wszystkie ciągi $(k_1, \ldots, k_l)$ nieujemnych liczb całkowitych takich, że

$$\varphi(p_1^{k_1}) \cdots \varphi(p_l^{k_l}) = m.$$

Każdemu takiemu ciągowi odpowiada rozwiązanie $n = p_1^{k_1} \cdots p_l^{k_l}$. Kluczowe jest opracowanie metody, która pozwoli znajdować takie ciągi w sposób efektywny i zarazem gwarantujący, że żadne możliwości nie zostaną pominięte.

Metoda

Omówimy teraz dokładniej metodę będącą konsekwencją powyższych obserwacji.

(1) Wyznaczamy wszystkie dzielniki (dodatnie) $d_1, \ldots, d_r$ liczby m, a następnie spośród liczb $d_1 + 1, \ldots, d_r + 1$ wybieramy wszystkie liczby pierwsze $p_1, \ldots, p_l$, przy czym zakładamy, że $p_1 > \cdots > p_l$. W szczególności, $p_l = 2$.

(2) Tworzymy pomocniczą tabelę, której kolumny indeksowane są liczbami pierwszymi $p_1, \ldots, p_l$, a wiersze nieujemnymi liczbami całkowitymi. Na przecięciu kolumny indeksowanej liczbą p oraz wiersza k wpisujemy wartość funkcji Eulera $\varphi(p^k)$. Obliczając wartości funkcji $\varphi(p^k)$, warto skorzystać z następujących rekurencyjnych wzorów:

$$\varphi(p^0) = 1, \tag{2.4}$$
$$\varphi(p^1) = p - 1, \tag{2.5}$$
$$\varphi(p^k) = p \cdot \varphi(p^{k-1}), \qquad \text{gdy } k > 1. \tag{2.6}$$

Wypełnianie kolumny odpowiadającej liczbie pierwszej p kończymy, gdy $\varphi(p^k)$ nie jest dzielnikiem liczby m.

(3) Tworzymy drzewo, z którego odczytamy ciągi, o których mowa w punkcie (T2).

- W korzeniu drzewa (jedynym wierzchołku na poziomie 1) wpisujemy liczbę m.

- Jeśli na poziomie i ($1 \leq i < l$) mamy wierzchołek v z wpisaną liczbą d, to z wierzchołka v rysujemy krawędzie, których etykietami są nieujemne liczby całkowite k takie, że $\varphi(p_i^k)$ dzieli e (w tym miejscu przydają się wartości funkcji Eulera policzone w punkcie (2). W wierzchołku kończącym rysowaną krawędź, który znajduje się na poziomie $i+1$, wpisujemy liczbę $\frac{d}{\varphi(p_i^k)}$.
- Jeśli v jest wierzchołkiem na poziomie l z wpisaną liczbą d, to możemy mieć do czynienia z jedną z następujących dwóch sytuacji:
  - jeśli nie istnieje $k \in \mathbb{N}$ takie, że $\varphi(2^k) = d$, to rysujemy krawędź zakończoną wierzchołkiem, w którym wpisujemy znak $\times$;
  - w przeciwnym wypadku (tzn. gdy d jest potęgą dwójki) dla każdego $k \in \mathbb{N}$ takiego, że $\varphi(2^k) = d$ (z wyjątkiem sytuacji, gdy $d = 1$, jest dokładnie jedno takie k; gdy $d = 1$, to mamy dwie możliwości dla k: 0 i 1) rysujemy krawędź z etykietą k zakończoną wierzchołkiem znajdującym się na poziomie $l+1$ z wpisaną liczbą 1.
- Na zakończenie dla każdego wierzchołka v z poziomu $l+1$ z wpisaną liczbą 1 odczytujemy (od góry) etykiety $k_1, \ldots, k_l$ krawędzi prowadzących od korzenia do v: każdy taki ciąg daje nam rozwiązanie
$$p_1^{k_1} \cdots p_l^{k_l}.$$

Przykład

Znajdziemy wszystkie dodatnie liczby całkowite n takie, że $\varphi(n) = 18$.

(1) Dzielnikami liczby 18 są
$$1, 2, 3, 6, 9, 18.$$
Po dodaniu do nich 1 otrzymujemy liczby
$$2, 3, 4, 7, 10, 19.$$
Po usunięciu liczb złożonych i uporządkowaniu od największej do najmniejszej, otrzymujemy liczby pierwsze
$$19, 7, 3, 2.$$

(2) Sporządzimy teraz tabelę zawierającą wartości funkcji Eulera dla potęg liczb 19, 7, 3, 2. Kolumny tabeli indeksowane są liczbami 19, 7, 3 i 2, a jej wiersze nieujemnymi liczbami całkowitymi.

Zgodnie ze wzorem (2.4) w „zerowym" wierszu tabeli wpisujemy jedynki i otrzymujemy następującą postać tabeli:

	19	7	3	2
0	1	1	1	1

Korzystając ze wzoru (2.5), w wierszu „pierwszym" w kolumnie odpowiadającej liczbie p wpisujemy liczbę $p-1$, co daje nam tabelę

	19	7	3	2
0	1	1	1	1
1	18	6	2	1

Przy wypełnianiu kolejnych wierszy korzystamy ze wzoru (2.6), co oznacza, że wierszu „k-tym" w kolumnie odpowiadającej liczbie p wpisujemy wartość z poprzedniego wiersza z tej samej kolumny pomnożoną przez p. W szczególności, dodając wiersz „drugi", dostajemy tabelę

	19	7	3	2
0	1	1	1	1
1	18	6	2	1
2	342	42	6	2

Zauważmy jednak, że 342 i 42 nie są dzielnikami 18, co zaznaczamy stawiając w odpowiednich miejscach krzyżyki:

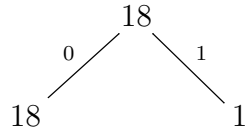
	19	7	3	2
0	1	1	1	1
1	18	6	2	1
2	~~342~~	~~42~~	6	2

(w oczywistych przypadkach – jak powyższe – możemy stawiać krzyżyki bez konieczności liczenia odpowiedniej wartości). Kontynuując powyższą procedurę i pomijając kolumny, w których postawiliśmy krzyżyki, otrzymujemy tabelę:

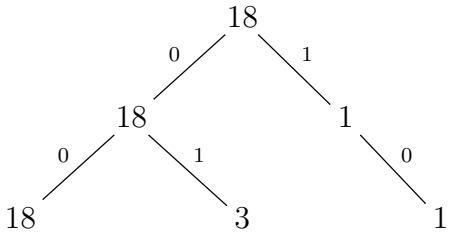
	19	7	3	2
0	1	1	1	1
1	18	6	2	1
2	~~342~~	~~42~~	6	2
3			18	~~1~~
4			×	

(3) Stworzymy teraz odpowiednie drzewo. Na początek tworzymy korzeń zawierający liczbę 18, tj. mamy następujące drzewo z jednym wierzchołkiem:

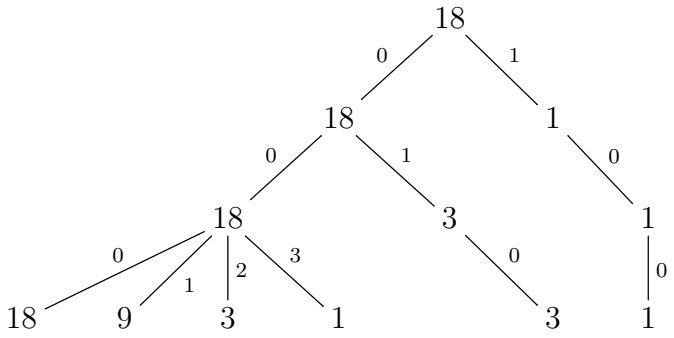
Następnie odczytujemy z tabeli sporządzonej w poprzednim kroku dla jakich k wartość $\varphi(19^k)$ dzieli 18 (tj. liczbę w korzeniu). Są to oczywiście $k = 0$ i $k = 1$. Będziemy zatem mieli dwie krawędzie z etykietami 0 i 1 wychodzące z korzenia, na końcu krawędzi z etykietą 0 wstawiamy liczbę $\frac{18}{\varphi(19^0)} = 18$, zaś na końcu krawędzi z etykietą 1 wstawiamy liczbę $\frac{18}{\varphi(19^1)} = 1$:



Teraz dla dwóch wierzchołków z poziomu 2 rysujemy krawędzie odpowiadające wykładnikom k, dla których $\varphi(7^k)$ dzieli odpowiednią liczbę, a więc mamy krawędzie dla $k = 0$ i $k = 1$ dla 18 i krawędź dla $k = 0$ dla 1:

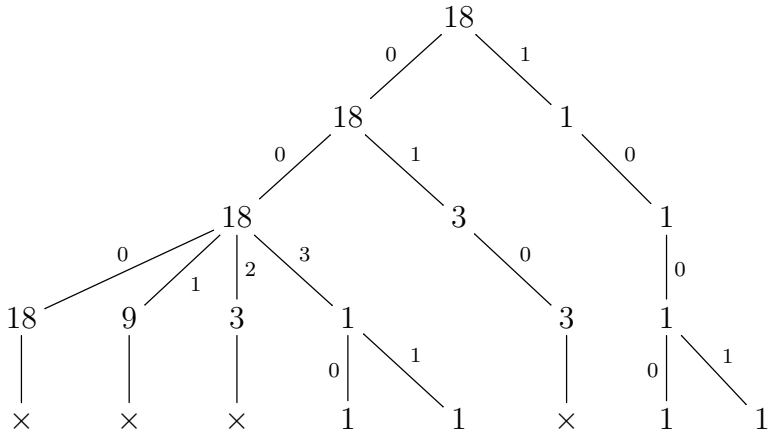


Powtarzając powyższe rozważania dla liczby pierwszej 3, otrzymujemy drzewo:



W ostatnim etapie analizujemy wartości funkcji Eulera dla potęg liczby pierwszej 2. W tym wypadku interesuje nas jednak dokładne dopasowanie. Ponieważ 18, 9 i 3 nie są wartościami funkcji Eulera dla potęg

dwójki, więc w tych wypadkach rysujemy krawędź (bez etykiety) zakończoną krzyżykiem ($\times$). Z drugiej strony, $\varphi(2^k) = 1$ dla $k = 0$ i $k = 1$, więc z wierzchołków z 1 wychodzą po dwie krawędzie z etykietami 0 i 1, odpowiednio:



Dla wierzchołków z najniższego poziomu z 1 wypisujemy ciągi etykiet krawędzi prowadzących z korzenia. Są to:

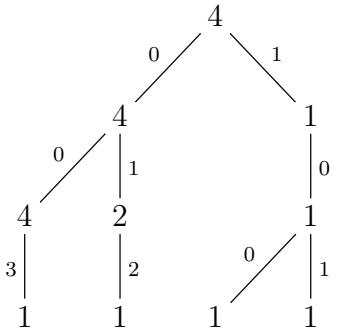
$$(0,0,3,0),\ (0,0,3,1),\ (1,0,0,0),\ (1,0,0,1).$$

Pamiętając, że poszczególne współrzędne odpowiadając liczbom pierwszym 19, 7, 3 i 2, odpowiednio, otrzymujemy liczby

$$19^0 \cdot 7^0 \cdot 3^3 \cdot 2^0 = 27,\ 19^0 \cdot 7^0 \cdot 3^3 \cdot 2^1 = 54,$$
$$19^1 \cdot 7^0 \cdot 3^0 \cdot 2^0 = 19,\ 19^1 \cdot 7^0 \cdot 3^0 \cdot 2^1 = 38.$$

2.1 Dodatkowy przykład drzewa

Dla $m = 4$ odpowiednie drzewo ma postać:



Zatem $\varphi(n) = 4$ dla

$$n \in \{5^0 \cdot 3^0 \cdot 2^3, 5^0 \cdot 3^1 \cdot 2^2, 5^1 \cdot 3^0 \cdot 2^0, 5^1 \cdot 3^0 \cdot 2^1\}.$$

Odpowiedzi do Zadania 2

(1) $n \in \varnothing$.

(2) $n \in \{15, 16, 20, 24, 30\}$.

(3) $n \in \{13, 21, 26, 28, 36, 42\}$.